Mobile Banking Security Tips

Do...

- Set a strong account password that has at least one number and capitalized letter. Do not use your name, birth date or other easily identifiable personal information in your password to avoid hacking. Try to change your password frequently. We recommend no less frequently than every 90 days.
- Always secure your phone with a password. If your phone is ever lost or stolen, it can help protect your private and secure information.
- Only download applications from trusted sources. Make sure to download updates regularly as often times these include fixes to security flaws.
- Keep the operating system on your phone updated.
- Use your mobile phone's security features. Enable encryption and remote wipe capabilities if available. Consider using additional security software and antivirus solutions that may be available for your type of mobile phone. (Refer to your phone's user manual or contact your mobile provider for more information on these features.)
- Read an application's privacy policy to be aware of what they are doing with your private information.
- Take note of pop-up notices and other alerts that may be warning you about security issues or leaving trusted sites.
- Delete text messages from your bank once you've read them.
- Always log off completely after using a mobile banking site or application.
- Make sure to clear out all information on your phone before discarding it.
- If you lose your mobile device or change your mobile phone number, remove the old number from your mobile banking profile.
- Be aware of your surroundings. Never leave your phone where others may be able to view incoming texts or pop-up alerts that may include sensitive information.

Don't…

- Send your personal information or online banking credentials via e-mail or text, as both are easy to intercept.
- Enter personal information unless there's an "s" after http, which indicates that the site is secure. Also, look for security symbols such as an icon of a lock.
- Bank or shop online while on a smartphone when using unsecured, public WiFi access.
- Set your phone settings to auto-fill User ID's or Password information.
- Click on any links in e-mails that claim to be from your bank. Instead go to your bank's website directly to log in.
- Do not hack your device (also known as Jailbreaking) as this can leave it open to infection from a virus or Trojan.